図５に示した携帯電話機１００の構成と異なる点は、まず、メモリカード１８０が装着されていること以外に、携帯電話機１０１は、公開暗号化キーＫＰｐを保持して、再生モード時にキーＫＰｐをデータバスＢＳ２に出力するＫＰｐ保持部１５２４を備える構成となっていることである。

さらに、携帯電話機１０１は、秘密復号キーＫｐを保持するＫｐ保持部１５２０と、このＫｐ保持部１５２０から与えられるキーＫｐに基づいて、データバスＢＳ２を介してメモリカード１８０から与えられるキーＫＰｐで暗号化されたセッションキーＫｓ１を復号し抽出する復号処理部１５２２とをさらに備える構成となっている。しかも、暗号化処理部１５０４は、この復号処理部１５２２から与えられるセッションキーＫｓ１により、Ｋｓ発生部１５０２からの自身のセッションキーＫｓを暗号化してデータバスＢＳ２に出力する。

携帯電話機１０１のその他の点は、図５に示した実施例１の携帯電話機１００の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図２７は、実施例７のメモリカード１８０に対応したコンテンツサーバ１１の構成を示す概略ブロック図である。図３に示したコンテンツサーバ１０の構成と異なる点は、データ処理部３１０における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓにより暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、セッションキーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介して通信装置３５０に与える点である。

コンテンツサーバ１１のその他の点は、図３に示した実施例１のコンテンツサーバ１０の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図２８は、本発明の実施例７のメモリカード１８０の構成を説明するための概略ブロック図であり、実施例４の図１８と対比される図である。

メモリカード１８０の構成が、メモリカード１５０の構成と異なる点は、まず、セッションキーＫｓ１発生部１４３２は、このカード独自のセッションキーＫｓ

１を発生することである。

メモリカード１８０は、さらに、カードという媒体に固有の公開暗号化キーＫＰｍｅｄｉａを保持するＫＰｍｅｄｉａ保持部１４４０の出力と、データバスＢＳ３を介して携帯電話機１０１から与えられる公開暗号化キーＫＰｐとを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ１４３６を備える。切換えスイッチ１４３６は、接点ＰｉおよびＰｈとを有し、接点ＰｉはデータバスＢＳ３と、接点ＰｈはＫＰｍｅｄｉａ保持部１４４０とそれぞれ結合する。暗号化処理部１４３０は、切換えスイッチ１４３６から与えられる公開暗号化キーＫＰｍｅｄｉａまたは公開暗号化キーＫＰｐのいずれかにより、Ｋｓ１発生部１４３２からのセッションキーＫｓ１を暗号化して、データバスＢＳ３に与える。

すなわち、切換えスイッチ１４３６は、配信モードのとき、および移動モードにおいて移動先となっているときは、未使用状態であり、再生モードの時は、接点Ｐｉの側に閉じており、移動モードにおいて移動元となっているときは、接点Ｐｈの側に閉じている。

メモリカード１８０は、さらに、接点Ｐｅ、ＰｆおよびＰｇを有し、復号処理部１４０４から与えられるコンテンツサーバ１１からのセッションキーＫｓと、Ｋｓ１発生部１４３２の出力と、データバスＢＳ４から与えられる携帯電話機１０１からのセッションキーＫｓとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４３５を、切換えスイッチ１４３４の替わりに備える。接点Ｐｅには復号処理部１４０４からの出力が、接点ＰｆにはＫｓ１発生部１４３２の出力が、接点ＰｇにはデータバスＢＳ４がそれぞれ結合している。したがって、暗号化処理部１４０６と復号処理部１４１０は、この切換えスイッチ１４３５から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

すなわち、切換えスイッチ１４３５は、配信モードの場合にコンテンツサーバ１１からのセッションキーの抽出を行なうときは、接点Ｐｅの側に閉じており、配信モードの場合に配信サーバからの暗号化されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤについてキーＫｓ１による復号を行なうときは、接点Ｐｆの側に閉じている。切換えスイ

ッチ１４３５は、再生モードにおいて復号処理を行なうときは、接点Ｐｆの側に閉じており、再生モードにおいて暗号化処理を行なうときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動モードにおいて移動元となっている場合に復号処理を行うときは、接点Ｐｆの側に閉じており、移動モードにおいて移動元となっている場合に暗号化処理を行うときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動モードにおいて移動先となっている場合に移動元のセッションキーを受け取るときは、接点Ｐｅの側に閉じており、移動モードにおいて移動先となっている場合にライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤを受け取るときは、接点Ｐｆの側に閉じている。

メモリカード１８０は、さらに、接点Ｐａ、Ｐｂ、ＰｃおよびＰｅを有し、Ｋｓ１発生部１４３２から与えられる自身のセッションキーＫｓｌと、ＫＰｃａｒｄ保持部１４０５の出力と、データバスＢＳ５から与えられるライセンスキーＫｃと、暗号化処理部１４１４から与えられ、相手方の公開暗号化キーＫＰｃａｒｄ（ｎ）により暗号化されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４０９を、切換えスイッチ１４０８の替わりに備える。接点ＰａにはＫｓ１発生部１４３２からの出力が、接点ＰｂにはＫＰｃａｒｄ保持部１４０５の出力が、接点ＰｃにはデータバスＢＳ５が、接点Ｐｄには暗号化処理部１４１４の出力が、それぞれ結合している。したがって、暗号化処理部１４０６は、この切換えスイッチ１４０９から与えられるデータに対して、それぞれ、暗号化処理を行なう。

すなわち、切換えスイッチ１４０９は、配信モードにおいて、配信先となっている場合にコンテンツサーバ１１に自身の公開暗号化キーＫＰｃａｒｄ（ｌ）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。切換えスイッチ１４０９は、再生モードのときは、接点Ｐｃの側に閉じており、移動モードにおいて移動元となっているときは、接点Ｐｄの側に閉じている。切換えスイッチ１４０９は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化キーＫＰｃａｒｄ（ｌ）や自身のセッ

ションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。

図２９は、図２８で説明したメモリカード１８０を用いた配信モードを説明するためのフローチャートである。

図２８においては、ユーザ１が、メモリカード１８０を用いることで、コンテンツサーバ１１からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１０１から、ユーザのタッチキー１１０８の操作等によって、コンテンツサーバ１１に対して配信リクエストがなされる（ステップＳ１００）。

コンテンツサーバ１１においては、この配信リクエストに応じて、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ１０３）。一方、メモリカード１８０の側では、Ｋｓ１発生部１４３２がセッションキーＫｓ１を生成する（ステップＳ１０３´）。

コンテンツサーバ１１では、続いて、コンテンツサーバ１１内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓを暗号化処理して、データバスＢＳ１に与える（ステップＳ１０４）。

通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを、通信網を通じて、携帯電話機１０１のメモリカード１８０に対して送信する（ステップＳ１０６）。

メモリカード１８０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１０８）。

続いて、配信モードにおいては、まず、切換えスイッチ１４０９が接点Ｐｂが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（ユーザ１のメモリカードにおける公開暗号化鍵）を受け取り、続いて、切換えスイッチ１４０９が接点Ｐａが閉じる状態となって、暗号化処理部１４０６は、接点Ｐａを介してＫｓ１保持部１４３２から与えられるセッションキーＫ

ｓ１を受け取る。暗号化処理部１４０６は、切換えスイッチ１４３５が接点Ｐｅが閉じる状態が選択されているので、復号処理部１４０４からのセッションキーＫｓにより、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化してデータバスＢＳ３に与える。

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓをコンテンツサーバ１１に対して出力する（ステップＳ１１２）。

サーバ３１では、通信装置３５０により受信され、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号化処理して、公開暗号化キーＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１１４）。

続いて、配信制御部３１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１１６）、かつ、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを生成する（ステップＳ１１８）。

暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを受取って、復号処理部３１８より与えられた公開暗号化キーＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１２０）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータを受取って、さらにセッションキーＫｓ１により暗号化して、データバスＢＳ１に与える（ステップＳ１２２）。

通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）］Ｋｓ１をカード１８０に対して送信する。

カード１８０においては、切換えスイッチ１４３５が接点Ｐｉが閉じる状態が選択される状態に切換えられているので、復号処理部１４１０は、Ｋｓ１発生部１４３２からのセッションキーＫｓ１により、復号処理を行ない、データ［ＫＣ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を抽出し（ステップ

Ｓ１２６），メモリ１４１２に格納する（ステップＳ１２８）。

さらに、メモリカード１８０においては、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を復号し、復号されたデータＬｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤをコントローラ１４２０が、レジスタ１５００に格納する（ステップ１２９）。

一方、コンテンツサーバ１１は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１８０に送信する（ステップＳ１３０）。

メモリカード１８０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

以上のような動作により、メモリカード１８０は、コンテンツデータを再生可能な状態となる。

図３０は、携帯電話機１０１内において、実施例７のメモリカード１８０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明するフローチャートである。

図３０を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１８０に対して出力される（ステップＳ２００）。

メモリカード１８０では、コントローラ１４２０がレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ，ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ２０５）。

コントローラ１４２０は、復号化されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップＳ２０６），再生可能回数を超えていないと判断した場合は、携帯電話機１０１のコントローラ１１０６に対して、再生許可通知を送信する（ステップＳ２０８）。

携帯電話機１０１においては、まず、公開暗号化キーＫＰｐをメモリカード１８０に対して送信し、セッションキー発生回路１５０２がセッションキーＫｓを

生成する（ステップＳ２１０）。

一方、メモリカード１８０でもセッションキーＫｓ１を生成し（ステップＳ２１０´）、公開暗号化キーＫＰｐでセッションキーＫｓ１を暗号化して（ステップＳ２１１）、携帯電話機１０１に暗号化セッションキー［Ｋｓ１］Ｋｐを送信する（ステップＳ２１２）。

携帯電話機１０１では、復号処理部１５２２が秘密復号キーＫｐにより、データバスＢＳ２を介してメモリカード１８０から与えられた暗号化セッションキー［Ｋｓ１］Ｋｐを復号し、セッションキーＫｓ１を抽出し（ステップＳ２１３）、暗号化処理部１５０４が、セッションキーＫｓ１によりセッションキーＫｓを暗号化して（ステップＳ２１４）、データバスＢＳ２に暗号化セッションキー［Ｋｓ］Ｋｓ１が出力される（ステップＳ２１５）。

メモリカード１８０は、データバスＢＳ３を介して、携帯電話機１０１により生成された暗号化セッションキー［Ｋｓ］Ｋｓ１を受け取り、セッションキーＫｓ１により復号し、セッションキーＫｓを抽出する（ステップＳ２１６）。

さらに、メモリカード１８０は、再生処理が行われることに応じて、レジスタ１５００中のライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤのうち、再生処理の累算数に関するデータを更新する（ステップ２１７）。

続いて、メモリカード１８０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号してライセンスキーＫｃを抽出する（ステップＳ２１８）。

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２１９）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２２０）。

携帯電話機１０１の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２２）。

続いて、メモリカード１８０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２４）。

携帯電話機の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、

抽出されたライセンスキーＫｃにより復号処理し（ステップＳ２２６）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ２２８）。

一方、ステップＳ２０６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード１８０は、携帯電話機１０１に対して、再生不許可通知を送信する（ステップＳ２３０）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図３１は、実施例７の２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図３１を参照して、まず、図３１においては、携帯電話機１０１が送信側であり、これと同様の構成を有する携帯電話機１０３が受信側であるものとする。また、携帯電話機１０３にも、メモリカード１８０と同様の構成を有するメモリカード１８２が装着されているものとする。

携帯電話機１０１は、まず、自身の側のメモリカード１８０と、受信側の携帯電話機１０３に挿入されたメモリカード１８２に対して、移動リクエストを出力する（ステップＳ３００）。

これに応じて、携帯電話機１０１においては、メモリカード１８０内のセッションキー発生回路１４３２は、セッションキーＫｓ１を生成し（ステップＳ３１２）、一方、携帯電話機１０３においては、メモリカード１８２内のセッションキー発生回路１４３２は、セッションキーＫｓ２を生成する（ステップＳ３１２´）。

携帯電話機１０１においては、メモリカード１８０は、公開暗号化キーＫＰｍｅｄｉａを用いて、暗号化処理部１４３０がセッションキーＫｓ１を暗号化して（ステップＳ３１４）、たとえば、トランシーバモードではアンテナ１１０２を介して、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａをメモリカード１８２に伝達する（ステップＳ３１６）。

メモリカード１８２においては、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより、セッションキーＫｓ１を復号抽出し（ステップＳ３２０）、さら

に、セッションキーＫｓ１によりメモリカード１８２の公開暗号化キーＫＰｃａｒｄ（２）およびセッションキーＫｓ２を暗号化して（ステップＳ３２２）、メモリカード１８０に対して、暗号化されたデータ［ＫＰｃａｒｄ（２）、Ｋｓ２］Ｋｓ１を送信する（ステップＳ３２４）。

メモリカード１８０においては、メモリカード１８２から送信された暗号化データを復号処理部１４１０がセッションキーＫｓ１により復号化して、メモリカード１８２の公開暗号化キーＫＰｃａｒｄ（２）およびセッションキーＫｓ２を復号抽出する（ステップＳ３２６）。このとき、切換えスイッチ１４３５では接点Ｐｆが閉じており、Ｋｓ１発生回路１４３２からのキーＫｓ１が復号処理部１４１０に与えられている。

続いて、メモリカード１８０においては、メモリ１４１２からメモリカード１５０の公開暗号化キーＫｃａｒｄ（１）により暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータUser－ＩＤが読出される（ステップＳ３２８）。

続いて、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤとを復号処理する（ステップＳ３３０）。

コントローラ１４２０は、このようにして復号されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３１）。

さらに、暗号化処理部１４１４は、復号処理部１４１０において抽出されたカード１８２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤとを暗号化する（ステップＳ３３２）。

暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ、Ｌｉｃｅｎｓｅ－ＩＤ、Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）をメモリカード１８２のセッションキーＫｓ２により暗号化する（ステップＳ３３４）。このとき、切換えスイッチ１４３５は、接点Ｐｇ

が閉じており，復号処理回路１４１０からのセッションキーＫｓ２が暗号化処理部１４０６に与えられている。

続いて、メモリカード１８０は，携帯電話機１０１を介して、メモリカード１８２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓ２を送信する（ステップＳ３３６）。

メモリカード１８２においては、メモリカード１８０から送信されたデータを復号処理部１４１０により、セッションキーＫｓ２に基づいて復号化処理して、メモリ１４１２に格納する（ステップＳ３３９）。さらに、メモリカード１８２は、ライセンスキーＫｃａｒｄ（２）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）を復号し、復号されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤをレジスタ１５００に格納する（ステップＳ３４１）。

一方、メモリカード１８０は、さらに、レジスタ１５００に格納されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤを消去する（ステップＳ３４３）。

続いて、メモリカード１８０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリから読出し、メモリカード１８２に対して送信する（ステップＳ３４４）。

メモリカード１８２は、受信した暗号化コンテンツデータをそのままメモリ１４１２に格納する（ステップＳ３４６）。

以上のような処理を行なうと、ステップＳ３４２において、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等がメモリカード１８０からは消去されているので、メモリカード１８０は「状態ＳＢ」となる。

一方、メモリカード１８２においては、暗号化コンテンツデータ以外にも、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のすべてのデータが移動されているので、メモリカード１８２は「状態ＳＡ」となっている。

以上のような構成を用いることで、たとえば、メモリカード１８０からメモリカード１８２へのデータの移動を、上述したようなセッションキー発生回路１５

０２を有する携帯電話機を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

しかも、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等は、レジスタ１５００に格納され、コントローラ１４２０はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティーが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤについては、メモリ１４１２に記録されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

〔実施例８〕

実施例８の携帯電話機１０５およびメモリカード１９０は、以下に説明するように、実施例７の携帯電話機１０１およびメモリカード１８０の構成とは、以下の点で異なることを特徴とする。

すなわち、実施例８の携帯電話機１０５では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機１０５を登録する際に、この携帯電話機１０５に割当てられた公開暗号化鍵ＫＰｐおよび認証データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

同様に、実施例８のメモリカード１９０でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード１９０を登録する際に、このメモリカードに割当てられた公開暗号化鍵ＫＰｍｅｄｉａおよび認証データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

ここで、メモリカード１９０および実施例８のコンテンツサーバ１２には、この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒを記録保持する手段を有している。この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒは、システム中でデータ出力を行なう全ての機器がセッションキーにやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号鍵の獲得に用いるシステム共通の鍵である。

以下、さらに、実施例８の携帯電話機１０５、メモリカード１９０およびコンテンツサーバ１２の構成をより詳しく説明する。

図３２は，実施例８における携帯電話機１０５の構成を説明するための概略ブロック図である。

図２６に示した携帯電話機１０１の構成と異なる点は、ＫＰｐ保持部１５２４の替わりに、公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された、公開暗号鍵ＫＰｐおよび認証データＣｒｔｆを保持するための[ＫＰｐ，Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１５２５を備える構成となっていることである。

携帯電話機１０５のその他の点は、図２６に示した実施例７の携帯電話機１０１の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３３は、実施例８のメモリカード１９０に対応したコンテンツサーバ１２の構成を示す概略ブロック図である。図２７に示したコンテンツサーバ１１の構成と異なる点は、データ処理部３１０は、公開復号鍵ＫＰｍａｓｔｅｒを保持するＫＰｍａｓｔｅｒ保持部３２４と、ＫＰｍａｓｔｅｒ保持部３２４から出力される公開復号キーＫＰｍａｓｔｅｒに基づいて、通信網から通信装置３５０を介してデータバスＢＳｌに与えられるデータを復号するための復号処理部３２６とをさらに備える構成となっている点である。暗号化処理部３１６は、復号処理部３２６での復号処理により抽出された公開暗号化キーＫＰｍｅｄｉａにより、Ｋｓ発生部３１４で発生されたセッションキーＫｓを暗号化し、また、配信制御部３１２は、復号処理部３２６での復号処理により抽出された認証データＣｒｔｆにより、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

コンテンツサーバ１２のその他の点は、図２７に示した実施例７のコンテンツサーバ１１の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３４は、本発明の実施例８のメモリカード１９０の構成を説明するための概略ブロック図であり、実施例７の図２８と対比される図である。

実施例８のメモリカード１９０の構成が、実施例７のメモリカード１８０の構成と異なる点は、まず、メモリカード１９０は、公開暗号鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する[ＫＰｍｅｄｉａ，Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２を備える構成となっていることである。一方で、切換えスイッチ１４３６は省略され、[ＫＰｍｅｄｉａ，Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２の出力は直接データバスＢＳ３に与えられる。

さらに、メモリカード１９０は、公開復号鍵ＫＰｍａｓｔｅｒを記録保持するためのＫＰｍａｓｔｅｒ保持部１４５０と、ＫＰｍａｓｔｅｒ保持部１４５０から出力される公開復号キーＫＰｍａｓｔｅｒに基づいて、データバスＢＳ３上のデータを復号するための復号処理部１４５２とを備える。

復号処理部１４５２での復号処理により抽出される公開暗号化鍵ＫＰｍｅｄｉａおよび認証データＣｒｔｆのうち、公開暗号化鍵ＫＰｍｅｄｉａは、暗号化処理部１４３０に与えられ、認証データＣｒｔｆは、データバスＢＳ５を介して、コントローラ１４２０に与えられる。

メモリカード１９０のその他の構成は、図２８に示したメモリカード１８０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３５は、図３４に示したメモリカード１９０内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊されるＴＲＭモジュールにより構成されるセキュリティー領域１４９０、ユーザからデータの存在は確認できるものの、そのデータがメモリカード固有の暗号化、ここでは公開暗号化鍵ＫＰｃａｒｄ（１）による暗号化が施され記録され、データの書き換えが自由に行なえない準セキュリティー領域１４９１と、コ

ーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティー領域１４９２とを備える。

セキュリティー領域１４９０には、メモリカード１９０の出荷時から保持する鍵の保持部、すなわち、Ｋｍｅｄｉａ保持部１４０２、ＫＰｃａｒｄ（１）保持部１４０５、Ｋｃａｒｄ（１）保持部１４１５、[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２、ＫＰｍａｓｔｅｒ保持部１４５０と、平文のライセンス情報が格納されるレジスタ１５００が設けられる。

準セキュリティー領域１４９１には、メモリカード１９００固有の暗号化をされたデータである[Ｋｃ，Ｌｉｓｅｎｃｅ－ＩＤ，Ｕｓｅｒ－ＩＤ]Ｋｃａｒｄ（１）が格納され、メモリ１４１２内に設けられる。

非セキュリティー領域１４９３には、暗号化コンテンツデータ[Ｄｃ]Ｋｃが格納され、メモリ１４１２内に設けられる。したがって、暗号化コンテンツデータ[Ｄｃ]Ｋｃは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。準セキュリティー領域１４９１に格納されたライセンス情報を他のメモリカードに複製しても、メモリカード１９００の固有の公開暗号鍵ＫＰｃａｒｄ（１）にてかけられた暗号化は、対の秘密復号鍵Ｋｃａｒｄ（１）を持たない他のメモリカードでは複製できないからである。

また、鍵を保持する全ての鍵保持部をセキュリティー領域に設けるよう説明したが、秘密復号鍵を保持するＫｍｅｄｉａ保持部１４０２およびＫｃａｒｄ（１）保持部１４１５のみセキュリティー領域に配置さえすれば良く、他の鍵保持部に保持された鍵は外部より参照できるＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）に配置されていてもよい。

図３６は、図３５で説明したメモリカード１９０を用いた配信モードを説明するためのフローチャートである。

図３６においては、ユーザ１が、メモリカード１９０を用いることで、コンテンツサーバ１２からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１０５から、ユーザのタッチキー１１０８の操作等によって、メモリカード１９０に対して配信リクエストがなされる（ステップＳ４００）。

メモリカード１９０からは、[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２から、携帯電話機１０５を経由して、コンテンツサーバ１２に対して，暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒが送信される（ステップＳ４０２）。

コンテンツサーバ１２においては、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒを受信すると、ＫＰｍａｓｔｅｒ保持部３２４が保持する公開復号キーＫＰｍａｓｔｅｒに基づいて、復号処理部３２６が復号処理することにより、公開暗号化キーＫＰｍｅｄｉａおよび認証データＣｒｔｆを取得する（ステップＳ４０４）。

さらに、コンテンツサーバ１２においては、認証データＣｒｔｆによりメモリカード１９０の認証を行ない（ステップＳ４０６）、メモリカード１９０が正規のメモリカードであることが証明されれば、処理はＳ４１２に移行する。一方、コンテンツサーバ１２は、メモリカード１９０が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し（ステップＳ４０８）、携帯電話機１０５が配信不許可通知を受信する（ステップＳ４１０）。

メモリカード１９０が正規のメモリカードであることが証明された場合、コンテンツサーバ１２では、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ４１２）。

コンテンツサーバ１２では、続いて、コンテンツサーバ１２内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓを暗号化処理して、データバスＢＳ１に与える（ステップＳ４１４）。

通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを、通信網を通じて、携帯電話機１０５のメモリカード１９０に対して送信する（ステップＳ４１６）。

メモリカード１９０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ４１８）。さらに、メモリカード１９０では、Ｋｓ１発生部１４３２がセッションキーＫｓ１を生成する（ステップＳ４２０）。

続いて、配信モードにおいては、まず、切換えスイッチ１４０９が接点Ｐｂが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を受け取り、続いて、切換えスイッチ１４０９が接点Ｐａが閉じる状態となって、暗号化処理部１４０６は、接点Ｐａを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１を受け取る。暗号化処理部１４０６は、切換えスイッチ１４３５が接点Ｐｅが閉じる状態が選択されているので、復号処理部１４０４からのセッションキーＫｓにより、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化してデータバスＢＳ３に与える（ステップＳ４２２）。

携帯電話機１０５を介して、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１），Ｋｓ１］Ｋｓがコンテンツサーバ１２に対して送信される（ステップＳ４２４）。

コンテンツサーバ１２では、通信装置３５０により受信され、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号化処理して、公開暗号化キーＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ４２６）。

続いて，配信制御部３１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ４２８）、かつ、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを生成する（ステップＳ４３０）。

暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを受取って、復号処理部３１８より与えられた公開暗号化キーＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ４３２）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータを受取って、さらにセッションキーＫｓ１により暗号化して、データバスＢＳ１に与える（ステップＳ４３４）。

通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，

Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）］Ｋｓ１をメモリカード１９０に対して送信する（ステップＳ４３６）。

メモリカード１９０においては、切換えスイッチ１４３５が接点Ｐｆが閉じる状態が選択される状態に切換えられているので、復号処理部１４１０は、Ｋｓ１発生部１４３２からのセッションキーＫｓ１により、復号処理を行ない、データ［ＫＣ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を抽出し（ステップＳ４３８）、メモリ１４１２に格納する（ステップＳ４４０）。

さらに、メモリカード１９０においては、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を復号し、復号されたデータＬｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤをコントローラ１４２０が、レジスタ１５００に格納する（ステップ４４２）。

一方、コンテンツサーバ１２は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１８０に送信する（ステップＳ４４４）。

メモリカード１９０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ４４６）。

以上のような動作により、メモリカード１９０は、コンテンツデータを再生可能な状態となる。

図３７は、携帯電話機１０５内において、実施例８のメモリカード１９０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明するフローチャートである。

図３７を参照して、携帯電話機のキーボード１１０８等からのユーザ１の指示により、再生リクエストが携帯電話機１０５に与えられると（ステップＳ５００）、携帯電話機１０５からメモリカード１９０に対して暗号化データ[ＫＰｐ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒが送信される（ステップＳ５０２）。

メモリカード１９０では、復号処理部１４５２での公開復号キーＫＰｍａｓｔｅｒによる復号処理により、公開暗号化鍵ＫＰｐおよび認証データＣｒｔｆが取得される（ステップＳ５０４）。コントローラ１４２０は、認証データＣｒｔｆにより携帯電話機１０５が正規の機器であるかを認証し（ステップＳ５０６）、

正規の機器であると証明されると、処理をステップＳ５０８に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機１０５に対して送信する（ステップＳ５４４）。

携帯電話機１０５が正規の機器であると証明された場合（ステップＳ５０６）、セッションキー発生部１４３２がセッションキーＫｓ１を生成する（ステップＳ５０８）。暗号化処理部１４３０は、復号処理部１４５２からの公開暗号化キーＫＰｐに基づいて、セッションキーＫｓ１を暗号化し（ステップＳ５１０）、暗号化セッションキー［Ｋｓ１］Ｋｐがメモリカード１９０から携帯電話機１０５に対して送信される（ステップＳ５１２）。

携帯電話機１０５では、復号処理部１５２２での復号処理により、セッションキーＫｓ１が復号され抽出される（ステップＳ５１４）。続いて、セッションキー発生部１５０２においてセッションキーＫｓが生成され（ステップＳ５１６）、暗号化処理部１５０４がセッションキーＫｓ１によりキーＫｓを暗号化して（ステップＳ５１８）、携帯電話機１０５からメモリカード１９０に対して、暗号化セッションキー［Ｋｓ］Ｋｓ１が送信される（ステップＳ５２０）。

メモリカード１９０では、復号処理部１４１０がセッションキーＫｓ１により、暗号化セッションキー［Ｋｓ］Ｋｓ１を復号処理してセッションキーＫｓを抽出する（ステップＳ５２２）。さらに、メモリカード１９０では、コントローラ１４２０がレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ５２４）。

コントローラ１４２０は、復号化されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップＳ５２６）、再生可能回数を超えていないと判断した場合は、メモリカード１９０は、再生処理が行われることに応じて、レジスタ１５００中のライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤのうち、再生処理の累算数に関するデータを更新する（ステップ５２８）。

続いて、メモリカード１９０は、メモリ１４１２から、暗号化されているデー

タ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を読出し、復号処理部１４１６が復号してライセンスキーＫｃを抽出する（ステップＳ５３０）。

続いて、ステップＳ５２２において抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ５３２）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ５３４）。

携帯電話機１０５の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ５３６）。

続いて、メモリカード１９０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ５３８）。

携帯電話機の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理し（ステップＳ５４０）、コンテンツデータを再生して混合部１５１０に与える（ステップＳ５４２）。

一方、ステップＳ５２６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード１９０は、携帯電話機１０５に対して、再生不許可通知を送信する（ステップＳ５４４）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図３８は、実施例８の２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図３８を参照して、まず、図３８においては、携帯電話機１０５が送信側であり、これと同様の構成を有する携帯電話機１０７が受信側であるものとする。また、携帯電話機１０７にも、メモリカード１９０と同様の構成を有するメモリカード１９２が装着されているものとする。

携帯電話機１０５は、まず、受信側の携帯電話機１０７に挿入されたメモリカード１９２に対して、移動リクエストを出力する（ステップＳ６００）。

これに応じて、携帯電話機１０７に装着されたメモリカード１９２からは、メモリカード１９０に対して、暗号化データ［ＫＰｍｅｄｉａ、Ｃｒｔｆ］ＫＰｍａ

ｓｔｅｒが送信される（ステップＳ６０２）。

メモリカード１９０においては、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒを受信すると、ＫＰｍａｓｔｅｒ保持部１４５０が保持する公開復号キーＫＰｍａｓｔｅｒに基づいて、復号処理部１４５２が復号処理することにより、公開暗号化キーＫＰｍｅｄｉａおよび認証データＣｒｔｆを取得する（ステップＳ６０４）。

さらに、メモリカード１９０においては、認証データＣｒｔｆによりメモリカード１９２の認証を行ない（ステップＳ６０６）、メモリカード１９２が正規のメモリカードであることが証明されれば、処理はＳ６１２に移行する。一方、メモリカード１９０は、メモリカード１９２が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し（ステップＳ６０８）、携帯電話機１０７が移動不許可通知を受信する（ステップＳ６１０）。

メモリカード１９２が正規のメモリカードであることが証明された場合、メモリカード１９０では、セッションキー発生部１４３２が、セッションキーＫｓ１を生成する（ステップＳ６１２）。

メモリカード１９０では、続いて、暗号化処理部１４３０が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓ１を暗号化処理して、データバスＢＳ３に与える（ステップＳ６１４）。

メモリカード１９０からは、暗号化処理部１４３０からの暗号化セッションキー[Ｋｓ]Ｋｍｅｄｉａを、携帯電話機１０５を通じて、携帯電話機１０７のメモリカード１９２に対して送信する（ステップＳ６１６）。

メモリカード１９２においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ６１８）。さらに、メモリカード１９２では、Ｋｓ１発生器１４３２と同様の構成を有するＫｓ２発生部１４３２´がセッションキーＫｓ２を生成する（ステップＳ６２０）。

続いて、メモリカード１９２では、まず、切換えスイッチ１４０９が接点Ｐｂが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐｂを介し

てＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を受け取り、続いて、切換えスイッチ１４０９が接点Ｐａが閉じる状態となって、暗号化処理部１４０６は、接点Ｐａを介してＫｓ２発生部１４３２´から与えられるセッションキーＫｓ２を受け取る。暗号化処理部１４０６は、切換えスイッチ１４３５が接点Ｐｅが閉じる状態が選択されているので、復号処理部１４０４からのセッションキーＫｓ１により、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ２を暗号化してデータバスＢＳ３に与える（ステップＳ６２２）。

携帯電話機１０７を介して、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１），Ｋｓ２］Ｋｓ１がメモリカード１９０に対して送信される（ステップＳ６２４）。

メモリカード１９０においては、メモリカード１９２から送信された暗号化データを復号処理部１４１０がセッションキーＫｓ１により復号化して、メモリカード１９２の公開暗号化キーＫＰｃａｒｄ（２）およびセッションキーＫｓ２を復号抽出する（ステップＳ６２６）。このとき、切換えスイッチ１４３５では接点Ｐｆが閉じており、Ｋｓ１発生回路１４３２からのキーＫｓ１が復号処理部１４１０に与えられている。

続いて、メモリカード１９０においては、メモリ１４１２から、メモリカード１９０の公開暗号化キーＫｃａｒｄ（１）により暗号化されているライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータUser－ＩＤが読出される（ステップＳ６２８）。

続いて、メモリカード１９０では、復号処理部１４１６が、秘密復号キーＫｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤとを復号処理する（ステップＳ６３０）。

メモリカード１９０のコントローラ１４２０は，このようにして復号されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤの値を、レジスタ１５００内のデータ値と置換する（ステップＳ６３２）。

さらに、メモリカード１９０の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１９２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤとを暗号化する（ステップＳ６３４）。

メモリカード１９０の暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）をメモリカード１９２のセッションキーＫｓ２により暗号化する（ステップＳ６３６）。このとき、切換えスイッチ１４３５は、接点Ｐｅが閉じており、復号処理回路１４１０からのセッションキーＫｓ２が暗号化処理部１４０６に与えられている。

続いて、メモリカード１９０は、携帯電話機１０５を介して、メモリカード１９２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓ２を送信する（ステップＳ６３８）。

メモリカード１９２においては、メモリカード１９０から送信されたデータを復号処理部１４１０により、セッションキーＫｓ２に基づいて復号化処理して、メモリ１４１２に格納する（ステップＳ６４０）。さらに、メモリカード１９２は、ライセンスキーＫｃａｒｄ（２）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）を復号し、復号されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤをレジスタ１５００に格納する（ステップＳ６４２）。

一方、メモリカード１９０は、さらに、レジスタ１５００に格納されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤを消去する（ステップＳ６４４）。

続いて、メモリカード１９０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、メモリカード１９２に対して送信する（ステップＳ６４６）。

メモリカード１９２は、受信した暗号化コンテンツデータをそのままメモリ１４１２に格納する（ステップＳ６４８）。

以上のような処理を行なうと、ステップＳ６４４において、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等がメモリカード１９０からは消去されているので、メモリカード１９０は「状態ＳＢ」となる。

一方、メモリカード１９２においては、暗号化コンテンツデータ以外にも、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等のすべてのデータが移動されているので、メモリカード１９２は「状態ＳＡ」となっている。

ここで、実施例７と同様に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等は、レジスタ１５００に格納され、コントローラ１４２０はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティーが一層向上する。

ここで、移動時には、再生情報内の再生回数を制限するライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤについては、メモリ１４１２に記録されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

［実施例９］

図３９は、実施例９のメモリカード２００の構成を示す概略ブロック図である。

実施例９のメモリカード２００は、以下に説明するように、実施例８のメモリカード１９０の構成とは、以下の点で異なることを特徴とする。

すなわち、実施例９のメモリカード２００では、実施例８のメモリカード１９０の構成において、Ｋｍｅｄｉａ保持部１４０２、ＫＰｃａｒｄ（１）保持部１４０５、Ｋｃａｒｄ（１）保持部１４１５、［ＫＰｍｅｄｉａ、Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２、ＫＰｍａｓｔｅｒ保持部１４５０およびレジスタ１５００が、メモリ１４１２の所定の領域内に設けられる構成となっている。こ

れに応じて、切換えスイッチ１４０９の接点ＰｂおよびＰｃが省略され、データバスＢＳ４とメモリ１４１２とは直接データのやり取りを行なわず、メモリ１４１２は、データバスＢＳ３との間でのみデータを授受するものとする。データバスＢＳ４は、データバスＢＳ３を介してメモリ１４１２とデータの授受を行なう。

図４０は、図３９に示したメモリカード２００内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊されるＴＲＭモジュールにより構成されるセキュリティー領域１４９０と、ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティー領域１４９２とを備える。

セキュリティー領域１４９０には、メモリカード２００の出荷時から保持する鍵の保持部、すなわち、Ｋｍｅｄｉａ保持部１４０２、ＫＰｃａｒｄ（１）保持部１４０５、Ｋｃａｒｄ（１）保持部１４１５、[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２、ＫＰｍａｓｔｅｒ保持部１４５０と、平文のライセンス情報が格納されるレジスタ１５００が設けられる。実施例８における図３５と異なるのは準セキュリティー領域が設けられていない点であり、このため準セキュリティー領域１４９１の格納されていた[Ｋｃ、Ｌｉｓｅｎｃｅ－ＩＤ、Ｕｓｅｒ－ＩＤ]Ｋｃａｒｄ（１）をＫｃａｒｄ（１）で復号した平文のライセンスキーＫｃ、ライセンスＩＤＬｉｓｅｎｃｅ－ＩＤ、ユーザＩＤＵｓｅｒ－ＩＤの内、実施例８においてレジスタ１５００に格納されていなかったコンテンツキーＫｃもセキュリティー領域１４９０に平文で格納される。このため、実施例８に比べてセキュリティー領域１４９０は、より広い記録空間が必要となる。

非セキュリティー領域１４９３には、暗号化コンテンツデータ[Ｄｃ]Ｋｃが格納され、メモリ１４１２がこれにあたる。したがって、暗号化コンテンツデータ[Ｄｃ]Ｋｃは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。

また、鍵を保持する全ての鍵保持部をセキュリティー領域に設けるよう説明したが、秘密復号鍵を保持するＫｍｅｄｉａ保持部１４０２およびＫｃａｒｄ（１）保持部１４１５のみセキュリティー領域に配置さえすれば良く、他の鍵保

持部に保持された鍵は外部より参照できるＲＯＭ（Read Only Memory）に配置されていても良い。

図４１は、図３９で説明したメモリカード２００を用いた配信モードを説明するためのフローチャートであり、実施例８の図３６と対比される図である。

図４１においては、ユーザ１が、メモリカード２００を用いることで、コンテンツサーバ１２からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１０５から、ユーザのタッチキー１１０８の操作等によって、メモリカード２００に対して配信リクエストがなされる（ステップＳ４００）。

メモリカード２００からは、メモリ１４１２中の[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部１４４２から、携帯電話機１０５を経由して、コンテンツサーバ１２に対して、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒが送信される（ステップＳ４０２）。

コンテンツサーバ１２においては、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒを受信すると、ＫＰｍａｓｔｅｒ保持部３２４が保持する公開復号キーＫＰｍａｓｔｅｒに基づいて、復号処理部３２６が復号処理することにより、公開復号キーＫＰｍｅｄｉａおよび認証データＣｒｔｆを取得する（ステップＳ４０４）。

さらに、コンテンツサーバ１２においては、認証データＣｒｔｆによりメモリカード２００の認証を行ない（ステップＳ４０６）、メモリカード２００が正規のメモリカードであることが証明されれば、処理はＳ４１２に移行する。

一方、コンテンツサーバ１２は、メモリカード２００が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し（ステップＳ４０８）、携帯電話機１０５が配信不許可通知を受信する（ステップＳ４１０）。

メモリカード２００が正規のメモリカードであることが証明された場合、コンテンツサーバ１２では、セッションキー発生部３１４が、セッションキーＫｓを生成する（ステップＳ４１２）。

コンテンツサーバ１２では、続いて、コンテンツサーバ１２内の暗号化処理部３１６が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓを暗号化

処理して、データバスＢＳ１に与える（ステップＳ４１４）。

通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを、通信網を通じて、携帯電話機１０５のメモリカード２００に対して送信する（ステップＳ４１６）。

メモリカード２００においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、データバスＢＳ３を介してメモリ１４１２から与えられる秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ４１８）。さらに、メモリカード２００では、Ｋｓ１発生部１４３２がセッションキーＫｓ１を生成する（ステップＳ４２０）。

続いて、配信モードにおいては、まず、暗号化処理部１４０６は、データバスＢＳ３を介してメモリ１４１２中のＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を受け取り、続いて、切換えスイッチ１４０９が接点Ｐａが閉じる状態となっているので、暗号化処理部１４０６は、接点Ｐａを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１を受け取る。暗号化処理部１４０６は、切換えスイッチ１４３５が接点Ｐｅが閉じる状態が選択されているので、復号処理部１４０４からのセッションキーＫｓにより、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化してデータバスＢＳ３に与える（ステップＳ４２２）。

携帯電話機１０５を介して、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓがコンテンツサーバ１２に対して送信される（ステップＳ４２４）。

コンテンツサーバ１２では、通信装置３５０により受信され、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号化処理して、公開暗号化キーＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ４２６）。

続いて、配信制御部３１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ４２８）、かつ、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよ

びユーザＩＤデータUser－ＩＤ等のデータを生成する（ステップＳ４３０）。

暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤおよびユーザＩＤデータ User－ＩＤ等のデータを受取って、復号処理部３１８より与えられた公開暗号化キーＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ４３２）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータを受取って、さらにセッションキーＫｓ１により暗号化して、データバスＢＳ１に与える（ステップＳ４３４）。

通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）］Ｋｓ１をメモリカード２００に対して送信する（ステップＳ４３６）。

メモリカード２００においては、切換えスイッチ１４３５が接点Ｐｉが閉じる状態が選択される状態に切換えられているので、復号処理部１４１０は、Ｋｓ１発生部１４３２からのセッションキーＫｓ１により、復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を抽出する（ステップＳ４３８）。

さらに、メモリカード２００においては、復号処理部１４１６が、メモリ１４１２中のＫｃａｒｄ（１）保持部１４１５からの出力に基づいて、復号処理部１４１０からのデータ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（１）を復号し、復号されたライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ，ユーザＩＤデータＵｓｅｒ－ＩＤ，ライセンスキーＫｃをメモリ１４１２中のレジスタ１５００に格納する（ステップ４４３）。

一方、コンテンツサーバ１２は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１８０に送信する（ステップＳ４４４）。

メモリカード２００においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ４４６）。

以上のような動作により、メモリカード２００は、コンテンツデータを再生可能な状態となる。

図４２は、携帯電話機１０５内において、実施例９のメモリカード２００に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートであり、実施例８の図３７と対比される図である。

図４１を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストが携帯電話機１０５に与えられると（ステップＳ５００）、携帯電話機１０５からメモリカード２００に対して暗号化データ[ＫＰｐ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒが送信される（ステップＳ５０２）。

メモリカード２００では、復号処理部１４５２での公開復号キーＫＰｍａｓｔｅｒによる復号処理により、公開暗号化鍵ＫＰｐおよび認証データＣｒｔｆが取得される（ステップＳ５０４）。コントローラ１４２０は、認証データＣｒｔｆにより携帯電話機１０５が正規の機器であるかを認証し（ステップＳ５０６）、正規の機器であると証明されると、処理をステップＳ５０８に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機１０５に対して送信する（ステップＳ５４４）。

携帯電話機１０５が正規の機器であると証明された場合（ステップＳ５０６）、セッションキー発生部１４３２がセッションキーＫｓ１を生成する（ステップＳ５０８）。暗号化処理部１４３０は、復号処理部１４５２からの公開暗号化キーＫＰｐに基づいて、セッションキーＫｓ１を暗号化し（ステップＳ５１０）、暗号化セッションキー［Ｋｓ１］Ｋｐがメモリカード２００から携帯電話機１０５に対して送信される（ステップＳ５１２）。

携帯電話機１０５では、復号処理部１５２２での復号処理により、セッションキーＫｓ１が復号され抽出される（ステップＳ５１４）。続いて、セッションキー発生部１５０２においてセッションキーＫｓが生成され（ステップＳ５１６）、暗号化処理部１５０４がセッションキーＫｓ１によりセッションキーＫｓを暗号化して（ステップＳ５１８）、携帯電話機１０５からメモリカード２００に対して、暗号化セッションキー［Ｋｓ］Ｋｓ１が送信される（ステップＳ５２０）。

メモリカード２００では、復号処理部１４１０がセッションキーＫｓ１により、暗号化セッションキー［Ｋｓ］Ｋｓ１を復号処理してセッションキーＫｓを抽出

する（ステップＳ５２２）。さらに、メモリカード２００では、コントローラ１４２０がメモリ１４１２中のレジスタ１５００からライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤ等を読出す（ステップＳ５２４）。

コントローラ１４２０は、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等に含まれる情報に基づいて、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップＳ５２６），再生可能回数を超えていないと判断した場合は、メモリカード２００は、再生処理が行われることに応じて、メモリ１４１２中のレジスタ１５００中のライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤのうち、再生処理の累算数に関するデータを更新する（ステップ５２８）。

続いて、メモリカード２００は、メモリ１４１２から、ライセンスキーＫｃを読出し、ステップＳ５２２において抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ５３２）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ５３４）。

携帯電話機１０５の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ５３６）。

続いて、メモリカード２００は、暗号化コンテンツキー［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスｂｓ２に与える（ステップＳ５３８）。

携帯電話機の音楽再生部１５０８は、暗号化コンテンツキー［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理し（ステップＳ５４０），コンテンツデータを再生して混合部１５１０に与える（ステップＳ５４２）。

一方、ステップＳ５２６において、コントローラ１４２０が復号処理は不可能であると判断した場合、メモリカード２００は、携帯電話機１０５に対して、再生不許可通知を送信する（ステップＳ５４４）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図４３は、実施例９の２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートであり、実施例８の図３８と対比される図である。

図４３を参照して、まず、図４３においては、携帯電話機１０５が送信側であり、これと同様の構成を有する携帯電話機１０７が受信側であるものとする。また、携帯電話機１０７にも、メモリカード２００と同様の構成を有するメモリカード２０２が装着されているものとする。

携帯電話機１０５は、まず、受信側の携帯電話機１０７に挿入されたメモリカード２０２に対して、移動リクエストを出力する（ステップＳ６００）。

これに応じて，携帯電話機１０７に装着されたメモリカード２０２からは、メモリカード２００に対して、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒが送信される（ステップＳ６０２）。

メモリカード２００においては、暗号化データ[ＫＰｍｅｄｉａ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒを受信すると、ＫＰｍａｓｔｅｒ保持部１４５０が保持する公開復号キーＫＰｍａｓｔｅｒに基づいて、復号処理部１４５２が復号処理することにより、公開暗号化キーＫＰｍｅｄｉａおよび認証データＣｒｔｆを取得する（ステップＳ６０４）。

さらに、メモリカード２００においては，認証データＣｒｔｆによりメモリカード２０２の認証を行ない（ステップＳ６０６）、メモリカード２０２が正規のメモリカードであることが証明されれば、処理はＳ６１２に移行する。一方、メモリカード２００は、メモリカード２０２が正規のメモリカードであることが証明されない場合は、移動不許可通知を送信し（ステップＳ６０８）、携帯電話機１０７が移動不許可通知を受信する（ステップＳ６１０）。

メモリカード２０２が正規のメモリカードであることが証明された場合、メモリカード２００では、セッションキー発生部１４３２が、セッションキーＫｓｌを生成する（ステップＳ６１２）。

メモリカード２００では、続いて、暗号化処理部１４３０が、公開暗号化キーＫＰｍｅｄｉａにより、セッションキーＫｓｌを暗号化処理して、データバスＢＳ３に与える（ステップＳ６１４）。

メモリカード２００からは、暗号化処理部１４３０からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａを、携帯電話機１０５を通じて、携帯電話機１０７のメモリカード２０２に対して送信する（ステップＳ６１６）。

メモリカード２０２においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号キーＫｍｅｄｉａにより復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ６１８）。さらに、メモリカード２０２では、Ｋｓ１発生器１４３２と同様の構成を有するＫｓ２発生部１４３２´がセッションキーＫｓ２を生成する（ステップＳ６２０）。

続いて、メモリカード２０２では、まず、暗号化処理部１４０６は、データバスＢＳ３を介してメモリ１４１２中のＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を受け取り、切換えスイッチ１４０９が接点Ｐａが閉じる状態となっているので、暗号化処理部１４０６は、接点Ｐａを介してＫｓ２発生部１４３２´から与えられるセッションキーＫｓ２を受け取る。暗号化処理部１４０６は、切換えスイッチ１４３５が接点Ｐｅが閉じる状態が選択されているので、復号処理部１４０４からのセッションキーＫｓ１により、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ２を暗号化してデータバスＢＳ３に与える（ステップＳ６２２）。

携帯電話機１０７を介して、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ２］Ｋｓ１がメモリカード２００に対して送信される（ステップＳ６２４）。

メモリカード２００においては、メモリカード２０２から送信された暗号化データを復号処理部１４１０がセッションキーＫｓ１により復号化して、メモリカード２０２の公開暗号化キーＫＰｃａｒｄ（２）およびセッションキーＫｓ２を復号抽出する（ステップＳ６２６）。このとき、切換えスイッチ１４３５では接点Ｐｆが閉じており、Ｋｓ１発生回路１４３２からのセッションキーＫｓ１が復号処理部１４１０に与えられている。

続いて、メモリカード２００では、メモリ１４１２中のレジスタ１５００から、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤ

データUser－ＩＤとが読み出される（ステップＳ６２９）。

さらに、メモリカード２００の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード２０２における公開暗号化キーＫＰｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータUser－ＩＤとを暗号化する（ステップＳ６３４）。

メモリカード２００の暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）をメモリカード２０２のセッションキーＫｓ２により暗号化する（ステップＳ６３６）。このとき、切換えスイッチ１４３５は、接点Ｐｇが閉じており、復号処理回路１４１０からのセッションキーＫｓ２が暗号化処理部１４０６に与えられている。

続いて、メモリカード２００は、携帯電話機１０５を介して、メモリカード２０２に対して、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）］Ｋｓ２を送信する（ステップＳ６３８）。

メモリカード２０２においては、メモリカード２００から送信されたデータを復号処理部１４１０により、セッションキーＫｓ２に基づいて復号化処理する（ステップＳ６４１）。さらに、メモリカード２０２は、秘密復号キーＫｃａｒｄ（２）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ－ＩＤ，Ｕｓｅｒ－ＩＤ］Ｋｃａｒｄ（２）を復号し、復号されたライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤをメモリ１４１２中のレジスタ１５００に格納する（ステップＳ６４３）。

一方、メモリカード２００は、レジスタ１５００よりライセンスキーＫｃ、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ、ユーザＩＤデータ User－ＩＤを消去し（ステップＳ６４４）、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、メモリカード２０２に対して送信する（ステップＳ６４６）。

メモリカード２０２は、受信した暗号化コンテンツデータをそのままメモリ１４１２に格納する（ステップＳ６４８）。

すなわち、以上のような構成でも、実施例８と同様の動作を実現できる。

なお、以上説明してきた各実施例において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権データや音楽サーバ３０に対するアクセス情報等を、付加情報Ｄｉとして暗号化コンテンツデータ併せて配信することも可能である。この付加データＤｉは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に記録される。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1．暗号化コンテンツデータを受けて記録するためのメモリカードであって、

前記メモリカードに対応して予め定められた第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記暗号化コンテンツデータの通信ごとに更新されて配信され、前記第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記メモリカードごとに異なる第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

前記第２の公開暗号化鍵を、前記第１の共通鍵に基づいて暗号化し、出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号化鍵で暗号化され、さらに前記第１の共通鍵で暗号化されたコンテンツキーを受け、前記第１の共通鍵に基づいて復号化するための第２の復号処理部（１４１０）と、

前記第２の復号処理部の出力を受けて、格納するための第１の記憶部（１４１２）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第１の記憶部に格納されたデータに基づいて、前記第２の秘密復号鍵により前記コンテンツキーを復号するための第３の復号処理部（１４１６）とを備える、メモリカード。

2．前記第１の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項１記載のメモリカード。

3．前記メモリカードは、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部（１４２０）をさらに備え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第３の復号処理部からの前記コンテンツキーを受けて、前記第１の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項２記載のメモリカード。

４．前記第２の復号処理部は、前記第２の公開暗号化鍵で暗号化され、さらに前記第１の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第１の共通鍵に基づいて復号し、

前記第３の復号処理部は、前記第２の復号処理部から与えられる、第１の共通鍵について復号され前記第２の公開暗号化鍵については暗号化された状態の前記ライセンス情報データを復号し、

前記第３の復号処理部からの復号された前記ライセンス情報データを格納するための第２の記憶部（１５００）をさらに備える、請求項３記載のメモリカード。

５．前記メモリカードは、

前記メモリカードに対応して予め定められた第１の公開暗号化鍵を保持し、外部に出力可能な第４の鍵保持部（１４４０）をさらに備える、請求項１記載のメモリカード。

６．前記第１の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項５記載のメモリカード。

７．前記メモリカードは、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御するための制御部をさらに備え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第３の復号処理部からの前記コンテンツキーを受けて、前記第１の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項６記載のメモリカード。

８．前記第２の復号処理部は、前記第２の公開暗号化鍵で暗号化され、さらに前

記第１の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第１の共通鍵に基づいて復号し、

前記第３の復号処理部は、前記第２の復号処理部から与えられる、第１の共通鍵について復号され前記第２の公開暗号化鍵については暗号化された状態の前記ライセンス情報データを復号し、

前記第３の復号処理部からの復号された前記ライセンス情報データを格納するための第２の記憶部をさらに備える、請求項７記載のメモリカード。

９．前記メモリカードは、

第２の共通鍵を生成するキーデータ生成部と、

前記第２の共通鍵を、前記第１の公開暗号化鍵によって暗号化するための第２の暗号化処理部とをさらに備え

暗号化された前記第２の共通鍵は、前記メモリカードから前記他のメモリカードに送信される、請求項１記載のメモリカード。

１０．前記メモリカードは、

少なくとも前記第１の暗号化処理部と、前記第１の復号処理部と、前記第２の復号処理部と、前記第３の復号処理部とが設けられ、第三者には読出不可能なセキュリティー領域（ＴＲＭ）と、

前記第１の記憶部が設けられ、第三者に読出可能なデータ領域とを備える、請求項２または６記載のメモリカード。

１１．前記メモリカードは、

少なくとも前記第１の暗号化処理部と、前記第１の復号処理部と、前記第２の復号処理部と、前記第３の復号処理部と、前記第２の記憶部とが設けられ、第三者には読出不可能なセキュリティー領域と、

前記第１の記憶部が設けられ、第三者に読出可能なデータ領域とを備える、請求項４または８記載のメモリカード。

１２．前記第１の記憶部は、前記暗号化コンテンツデータに付随した非暗号化データを、前記暗号化コンテンツデータとともに受けて格納する請求項２または６記載のメモリカード。

１３．暗号化データと前記暗号化データを復号するための復号情報データを受け

て記録するためのメモリカードであって、

前記暗号化データを格納する第１の記憶部（１４１２）と、

前記メモリカードに対応して予め定められた第１の公開暗号化鍵と自身の認証データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して出力可能な第１の鍵保持部（１４４２）と、

第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第２の鍵保持部（１４０２）と、

前記復号情報データの通信ごとに更新されて送信され、前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記メモリカードごとに異なる第２の公開暗号化鍵を保持するための第３の鍵保持部（１４０５）と、

前記復号情報データの通信ごとに更新される第２の共通鍵を生成するセッションキー発生部（１４３２）と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、出力するための第１の暗号化処理部（１４０６）と、

外部にて前記第２の公開暗号鍵によって暗号化され、さらに第２の共通鍵によって暗号化された前記復号情報データを前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記第２の復号処理部の出力である前記第２の公開暗号鍵によって暗号化された前記復号情報データを格納する第２の記憶部（１５００）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号するための第２の秘密復号鍵を保持する第４の鍵保持部（１４１５）と、

前記第２の記憶部に格納されたデータを前記第２の秘密復号鍵に基づいて復号し、前記復号情報データを抽出するための第３の復号処理部（１４１６）とを備える、メモリカード。

１４．前記メモリカードは、

前記公開認証鍵を保持する第４の鍵保持部（１４５０）と、

前記公開認証鍵によって復号できるように暗号化された外部から与えられる自

身以外の第３の公開暗号化鍵と、自身以外の第２の認証データを復号して抽出する第４の復号処理部（１４５２）と、

前記第４の復号処理部により抽出された前記第２の認証データに基づいて認証処理を行ない、認証できない場合、前記復号情報データの出力を禁止する制御部（１４２０）と、

前記セッションキー生成部にて通信ごとに更新した第２の共通鍵を、前記第３の公開暗号化鍵に基づいて暗号化して出力する第３の暗号化処理部（１４０６）と、

外部からの自身以外の固有の第４の公開暗号化鍵に基づいて暗号化を行なうための第３の暗号処理部（１４１４）をさらに備え、

外部からの復号情報データの出力要求があり、かつ、前記制御部が復号情報データの出力を禁止しない場合、

ｉ）　前記第２の復号処理部は、第２の共通鍵によって暗号化された前記第１の共通鍵、または第４の公開暗号化鍵および第１の共通鍵をさらに復号出力し、

ii）　前記第２の復号処理部にて前記第４の公開暗号化鍵が抽出された場合、前記第３の復号手段は、前記第１の記憶部に記録されたデータから復号情報データを抽出し、前記第３の暗号化処理部は、前記第３の復号処理部の出力を前記第２の復号処理部にて出力された第４の公開暗号化鍵にて暗号化して、さらに、第１の暗号化処理部は、第３の暗号化処理部の出力を前記第２の復号処理部にて抽出された第２の共通鍵に基づいて暗号化して出力し、

iii）　前記第２の復号処理部にて前記第２の共通鍵のみが抽出された場合、前記第２の復号処理手段は、前記第１の記憶部に格納されたデータから復号情報データを抽出し、前記第３の暗号化処理部は、前記第２の復号処理部の出力を、前記第２の復号処理部にて抽出された第２の共通鍵に基づいて暗号化出力する、請求項１３記載のメモリカード。

１５．前記復号情報データは、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データをさらに含み、

前記第３の復号部にて前記第２の公開暗号化鍵によって暗号かされた復号再生情報から抽出した前記アクセス制御情報を格納する第３の記憶部をさらに備え、

前記制御部は、前記第３の記憶部に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項１４記載のメモリカード。

１６．前記メモリカードの記録空間は、

第三者に読出不能かつ書替不可能なセキュリティ領域と、

第三者に読出可能であり、格納データはメモリカード固有の暗号化が施されている準セキュリティ領域と、

第三者に読出および書替可能な非セキュリティ領域とに区分され、

前記セキュリティ領域は、前記第１、第３の鍵保持部および第３の記憶部を含み、

前記準セキュリティ領域は、前記第２の記憶部を含み、

前記非セキュリティ領域は、第１の記憶部を含む、請求項１５記載のメモリカード。

１７．前記準セキュリティ領域および前記非セキュリティ領域は、同一メモリ上に配置される請求項１６記載のメモリカード。

１８．暗号化データと前記暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、

```
ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK:
```